

IN THE UNITED STATES DISTRICT COURT  
FOR THE NORTHERN DISTRICT OF OHIO  
WESTERN DIVISION

IN THE MATTER OF THE SEARCH OF  
INFORMATION ASSOCIATED WITH THE  
CELLULAR DEVICES ASSIGNED CALL  
NUMBER **(419) 604-1816**, THAT IS  
STORED AT PREMISES CONTROLLED  
BY **VERIZON WIRELESS**

Case Nos.: 3:21MJ5020  
3:21MJ5021  
3:21MJ5022

USDJ Nos. 21-6-001-TOL  
21-6-002-TOL  
21-6-003-TOL

**Filed Under Seal**

**AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT**

I, Andrew J. Eilerman, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application for a search warrant for information associated with a certain cellular telephone assigned call number, **(419) 604-1816 (hereafter referred to as Target Number)**, that is stored at a premises controlled by **Verizon Wireless**, a wireless telephone service provider headquartered at 180 Washington Valley Road, Bedminster, New Jersey 07921. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under Federal Rule of Criminal Procedure 41 and 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require **Verizon Wireless** to disclose to the government records and other information in its possession pertaining to the subscriber or customer associated with the accounts, including the contents of communications. Upon receipt of the information described in Section I

of Attachment B, government-authorized persons will review the information to locate items described in Section II of Attachment B.

2. Because this warrant seeks among other things the prospective collection of information, including cell-site location information, that may fall within the statutory definitions of information collected by a “pen register” and/or “trap and trace device,” *see* 18 U.S.C. § 3127(3) & (4), the requested warrant is designed to also comply with the Pen Register Act. *See* 18 U.S.C. §§ 3121-3127. The requested warrant therefore includes all the information required to be included in an order pursuant to that statute. *See* 18 U.S.C. § 3123(b)(1) and Attachment C.

3. I am a Special Agent of the Federal Bureau of Investigation (FBI), and, have been since May 2008. Your Affiant is currently assigned to the Cleveland Division, Lima Resident Agency. I worked in the same capacity in the Cincinnati Division, Dayton Resident Agency and the Minneapolis Division, Grand Forks, North Dakota Resident Agency. Your Affiant has investigated the commission of federal crimes involving criminal offenses and national security matters to include counterintelligence investigations, violent crimes, and drug trafficking. In the course of these duties, Your Affiant has participated in numerous federal search and arrest operations and conducted associated interviews which have resulted in the collection of evidence and admissions of multiple criminal violations. Additionally, Your Affiant has used cellular telephone information like electronic communications, historical and prospective location information to further investigations, including in drug trafficking investigation. I am familiar with such data and the interpretations of such data.

4. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other task force officers and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

5. Based on the facts set forth in this affidavit, there is probable cause to believe that violations of Title 21, U.S.C., Sections 841(a)(1) and 846 – Possession with the Intent to Distribute Narcotics and Drug Conspiracy have been committed, are being committed, and will be committed by individuals using the **Target Number**. There is also probable cause to believe that the location information described in Attachment B will constitute evidence of these criminal violations, and will lead to the identification of individuals who are engaged in the commission of these offenses.

### **JURISDICTION**

6. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is a district court of the United States that has jurisdiction over the offense being investigated. *See* 18 U.S.C. § 2711(3)(A)(i).

### **PROBABLE CAUSE**

7. The Federal Bureau of Investigation along with the West Central Ohio Crime Task Force (WCOCTF) has been conducting an investigation into a drug trafficking organization operating in Lima, Ohio with ties to both Toledo, Ohio and Cleveland, Ohio and other locations yet unknown. This drug trafficking organization is believed to be involved in the illegal sale of cocaine, crack cocaine, heroin and Fentanyl. Some of the most recent activities involving MICHELLE GODSEY (“MICHELLE”) and MATREVUS GODSEY (“MATREVUS”) are described below.

8. MICHELLE and MATREVUS are currently married. They recently moved their primary residence from 1840 West Breese Road, Lima, Ohio to 218 North Shawnee Street, Lima,

Ohio. Controlled drug buys<sup>1</sup> have been conducted at both locations. While, it appears that MICHELLE and MATREVUS are currently residing at 218 North Shawnee Street, Lima, Ohio, surveillance has placed them at the West Breese Road address as recent as January 19, 2021.

9. On December 03, 2020, the Federal Bureau of Investigation (FBI), while working with the WCOCTF, conducted a controlled drug purchase utilizing a WCOCTF Confidential Informant (CI). The drug buy was set up by having the CI<sup>2</sup> contact MARTREVUS, via the **Target Number**. The transaction was set up via a telephone call to the **Target Number**, and the CI purchased 2 grams of crack cocaine.

10. The controlled drug buy occurred at the GODSEY's residence located at 1840 West Breese Road, Lima, Ohio. MICHELLE and MATREVUS both utilize the **Target Number**. During this controlled buy, a male's voice was heard on the transmitter which the CI later identified as being MATREVUS. The narcotics purchased were field tested using a NIK test kit, which yielded a presumptive positive test for cocaine.

11. On December 4, 2020, the same CI contacted MATRAVUS, via a different cellular telephone number. The CI set up and purchased one gram of cocaine and one gram of fentanyl. The transaction occurred at the 1840 West Breese Road residence. The narcotics were field tested using a NIK test and the test results yielded a presumptive positive test for one of the substances purchased as fentanyl and the other as cocaine.

---

<sup>1</sup> During the controlled buys or purchases as mentioned in this affidavit, the confidential informant was given money and recording devices to buy the controlled substance. Prior to meeting with the targets, the confidential informant was searched for any contraband and law enforcement met them immediately after the transaction to seize the controlled substance.

<sup>2</sup> The confidential informant is being paid for his/her cooperation. He/she has worked with law enforcement in other investigations and his/her information has been deemed reliable.

12. Later that day on December 4, 2020, MICHELLE used **Target Number** and contacted the CI and asked the CI to travel with her to Findlay, Ohio, in order to sell illegal narcotics in the city of Findlay, Ohio. MICHELE informed the CI that she would pay the CI for their time and assistance. Investigators ultimately did not allow the CI to travel with MICHELLE for safety concerns.

13. On December 21, 2020, the CI contacted MICHELLE via the **Target Number**, both via text messages and telephone calls. The text messages are as follows (MG is MICHELLE):

CI: Wyd

CI: U up and around?

MG: Yup

CI: Did you ever get the hard in?

CI: My uncles bout to be in town

CI: Answer the phone sis

MG: Yea he wants

CI: He wants a g

CI: How much is that?

CI: Hard

MG: 125

CI: This shit so expensive (smiley face smiley face) I'm glad you only got me smoking weed and on the right track sis

CI: But if people around me ik imma just send them your way

MG: It's fire he will love it an I'm so happy your doin good did you start Nelson's yet

CI: I start Wednesday lol. And am I just coming to your house?

14. After meeting with members of the WCOCTF, the CI made a telephone call to MICHELLE via the **Target Number** to finalize the details of the transaction. This phone call was made in the presence of Task Force Officer (TFO) Aaron Montgomery. The CI asked MICHELLE where the drug transaction was going to occur. A mutual agreement was made that the transaction was going to occur in the retailer's parking lot on Allentown Road, Lima, Ohio.

15. The controlled drug buy was surveilled by members of the WCOCTF, and photos were taken of MICHELLE. The transaction was also monitored and recorded via a transmitter. The CI purchased one gram of crack cocaine. The substance was field tested via a NIK test that test yielded a presumptive positive test for cocaine.

16. On January 20, 2021, the same CI conducted a controlled narcotics buy from MICHELLE along with MATRAVUS present. The CI made a telephone call to **Target Number**, and had a conversation with MICHELLE. The CI was told that he/she could come to MICHELL's new residence located 218 North Shawnee Street, Lima, Ohio and make the purchase. The CI informed MICHELLE that he/she had \$200 to spend and requested to purchase crack cocaine.

17. During the controlled operation, the CI traveled to 218 North Shawnee Street, Lima, Ohio and purchased 2.2 grams (with the weight of the baggie) of crack cocaine. The substance was field tested via a NIK test that yielded a presumptive positive test for cocaine.

18. FBI personnel served a preservation letter to Verizon on January 7, 2021 requesting that they preserve text message data from December 31, 2020 through January 7, 2021. On January 21, 2021, Affiant contacted Verizon and confirmed that the data has been preserved.

19. Stored text messaging communication will assist investigators determine where the users of **Target Number** of travel and likely meeting spots in delivering and picking up illegal narcotics. This information may provide investigators with additional leads, and additional information/evidence regarding this drug trafficking organization's activities.

20. Records, data, messages, text messages, multi-media messages from Verizon Wireless will assist investigators with identifying who the user(s) of **Target Number** are supplying illegal narcotics to as well as assist in determining who their source of supply is. This information may provide investigators with additional leads, and additional information/evidence regarding this drug trafficking organization.

21. Similarly, historic and prospective location information will help determine physical locations that are linked to the trafficking of controlled substances like the storage of money and/or controlled substances, and help identify co-conspirators including the suppliers to the MICHELLE and MATRAVUS.

#### **Verizon Wireless – LOCATION/CELL SITE DATA**

22. In my training and experience, I have learned that **Verizon Wireless** is a company that provides cellular telephone access to the general public. I also know that providers of cellular telephone service have technical capabilities that allow them to collect and generate information about the locations of the cellular telephones to which they provide service, including cell-site data, also known as “tower/face information” or “cell tower/sector records.” Cell-site data

identifies the “cell towers” (i.e. antenna towers covering specific geographic areas) that received a radio signal from the cellular telephone and, in some cases, the “sector” (i.e. faces of the towers) to which the telephone connected. These towers are often a half-mile or more apart, even in urban areas, and can be 10 or more miles apart in rural areas. Furthermore, the tower closest to a wireless device does not necessarily serve every call made to or from that device. Accordingly, cell-site data provides an approximate location of the cellular telephone but is typically less precise than other types of location information, such as E-911 Phase II data or Global Positioning Device (“GPS”) data.

23. Based on my training and experience, I know that **Verizon Wireless** can collect cell-site data about the **Target Number**. I also know that wireless providers such as **Verizon Wireless** typically collect and retain cell-site data pertaining to cellular phones to which they provide service in their normal course of business in order to use this information for various business-related purposes.

24. Based on my training and experience, I know that Verizon also collects per-call measurement data, which Verizon also refers to as the “real-time tool” (“RTT”). RTT data estimates the approximate distance of the cellular device from a cellular tower based on the speed with which signals travel between the device and the tower. This information can be used to estimate an approximate location range that is more precise than typical cell-site data.

25. Based on my training and experience, I know that wireless providers such as **Verizon Wireless** typically collect and retain information about their subscribers in their normal course of business. This information can include basic personal information about the subscriber, such as name and address, and the method(s) of payment (such as credit card account number) provided by the subscriber to pay for wireless telephone service. I also know that wireless providers such as **Verizon Wireless** typically collect and retain information about their



subscribers' use of the wireless service, such as records about calls or other communications sent or received by a particular phone and other transactional records, in their normal course of business. In my training and experience, this information may constitute evidence of the crimes under investigation because the information can be used to identify the SUBJECT PHONE's user or users and may assist in the identification of co-conspirators and/or victims.

**Verizon Wireless – COMMUNICATION CONTENT**

26. In my training and experience, I have learned that **Verizon Wireless** is a company that provides cellular telephone access to the general public, and that stored electronic communications, including retrieved and unretrieved voicemail, text, and multimedia messages for **Verizon Wireless** subscribers may be located on the computers of **Verizon Wireless**. Further, I am aware that computers located at **Verizon Wireless** contain information and other stored electronic communications belonging to unrelated third parties.

27. Wireless phone providers often provide their subscribers with voicemail services. In general, a provider will store voicemail messages on behalf of a particular subscriber until the subscriber deletes the voicemail. If the subscriber does not delete the message, the message may remain in the system of **Verizon Wireless** for weeks or months.

28. Among the services commonly offered by wireless phone providers is the capacity to send short text or multimedia messages (photos, audio, or video) from one subscriber's phone or wireless device to another phone or wireless device via one or more wireless providers. This service is often referred to as "Short Message Service" ("SMS") or "Multimedia Messaging Service" ("MMS") and is often referred to generically as "text messaging." Based on my knowledge and experience, I believe that stored electronic communications, including SMS and

MMS messages that have been sent or received by subscribers, may be stored by **Verizon Wireless** for short periods incident to and following their transmission. In addition, providers occasionally retain printouts from original storage of text messages for a particular subscriber's account.

29. Wireless phone providers typically retain certain transactional information about the use of each telephone, voicemail, and text-messaging account on their systems. This information can include log files and messaging logs showing all activity on the account, such as local and long distance telephone connection records, records of session times and durations, lists of all incoming and outgoing telephone numbers or e-mail addresses associated with particular telephone calls, voicemail messages, and text or multimedia messages. Providers may also have information about the dates, times, and methods of connecting associated with every communication in which a particular cellular device was involved.

30. Wireless providers may also retain text messaging logs that include specific information about text and multimedia messages sent or received from the account, such as the dates and times of the messages. A provider may also retain information about which cellular handset or device was associated with the account when the messages were sent or received. The provider could have this information because each cellular device has one or more unique identifiers embedded inside it. Depending upon the cellular network and the device, the embedded unique identifiers for a cellular device could take several different forms, including an Electronic Serial Number ("ESN"), a Mobile Electronic Identity Number ("MEIN"), a Mobile Identification Number ("MIN"), a Subscriber Identity Module ("SIM"), an International Mobile Subscriber Identifier ("IMSI"), or an International Mobile Station Equipment Identity ("IMEI"). When a cellular device connects to a cellular antenna or tower, it reveals its embedded unique identifiers to the cellular antenna or tower in order to obtain service, and the cellular antenna or tower records those identifiers as a matter of course.

31. Many wireless providers retain information about the location in which a particular communication was transmitted or received. This information can include data about which “cell towers” (i.e., antenna towers covering specific geographic areas) received a radio signal from the cellular device and thereby transmitted or received the communication in question.

32. Wireless providers also maintain business records and subscriber information for particular accounts. This information could include the subscribers’ full names and addresses, the address to which any equipment was shipped, the date on which the account was opened, the length of service, the types of service utilized, the ESN or other unique identifier for the cellular device associated with the account, the subscribers’ Social Security Numbers and dates of birth, all telephone numbers and other identifiers associated with the account, and a description of the services available to the account subscribers. In addition, wireless providers typically generate and retain billing records for each account, which may show all billable calls (including outgoing digits dialed). The providers may also have payment information for the account, including the dates, times and sometimes, places, of payments and the means and source of payment (including any credit card or bank account number).

33. In some cases, wireless subscribers may communicate directly with a wireless provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Wireless providers typically retain records about such communications, including records of contacts between the user and the provider’s support services, as well records of any actions taken by the provider or user as a result of the communications.

34. As explained below, information stored at the wireless provider, including that described above, may provide crucial evidence of the “who, what, why, when, where, and how”

of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the data pertaining to a particular cellular device that is retained by a wireless provider can indicate who has used or controlled the cellular device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, data collected at the time of account sign-up, information relating to account payments, and communications (and the data associated with the foregoing, such as date and time) may indicate who used or controlled a cellular device at a relevant time. Further, such stored electronic data can show how and when the cellular device and associated cellular service were accessed or used. Such “timeline” information allows investigators to understand the chronological context of cellular device usage, account access, and events relating to the crime under investigation. This “timeline” information may tend to either inculcate or exculpate the cellular device owner. Additionally, information stored by the wireless provider may indicate the geographic location of the cellular device and user at a particular time (e.g., historic cell-site location information; location integrated into an image or video sent via text message to include both metadata and the physical location displayed in an image or video). Last, stored electronic data may provide relevant insight into the state of mind of the cellular device’s owner and/or user as it relates to the offense under investigation. For example, information relating to the cellular device in the possession of the wireless provider may indicate the owner’s motive and intent to commit a crime (e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement).

**INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED**

35. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require **Verizon Wireless** to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

**AUTHORIZATION REQUEST**

36. Based on the foregoing, I request that the Court issue the proposed search warrant, pursuant to 18 U.S.C. § 2703(c) and Federal Rule of Criminal Procedure 41.

37. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

38. I further request that the Court direct **Verizon Wireless** to disclose to the government any information described in Section I of Attachment B that is within its possession, custody, or control. Because the warrant will be served on **Verizon Wireless**, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

39. I further request, pursuant to 18 U.S.C. § 3103a(b) and Federal Rule of Criminal Procedure 41(f)(3), that the Court authorize the officer executing the warrant to delay notice until 30 days after the collection authorized by the warrant has been completed. There is reasonable cause to believe that providing immediate notification of the warrant may have an adverse result, as defined in 18 U.S.C. § 2705. Providing immediate notice to the subscriber or user of the

Target Cell Phone would seriously jeopardize the ongoing investigation, as such a disclosure would give that person an opportunity to destroy evidence, change patterns of behavior, notify confederates, and flee from prosecution. *See* 18 U.S.C. § 3103a(b)(1). As further specified in Attachment B, which is incorporated into the warrant, the proposed search warrant does not authorize the seizure of any tangible property. *See* 18 U.S.C. § 3103a(b)(2). Moreover, to the extent that the warrant authorizes the seizure of any wire or electronic communication (as defined in 18 U.S.C. § 2510) or any stored wire or electronic information, there is reasonable necessity for the seizure for the reasons set forth above. *See* 18 U.S.C. § 3103a(b)(2).

40. I further request that the Court direct **Verizon Wireless** to disclose to the government any information described in Section I of Attachment B that is within its possession, custody, or control. I also request that the Court direct **Verizon Wireless** to furnish the government all information, facilities, and technical assistance necessary to accomplish the collection of the information described in Attachment B unobtrusively and with a minimum of interference with **Verizon Wireless's** services, including by initiating a signal to determine the location of the Target Cell Phone on **Verizon Wireless's** network or with such other reference points as may be reasonably available, and at such intervals and times directed by the government. The government shall reasonably compensate **Verizon Wireless** for reasonable expenses incurred in furnishing such facilities or assistance.

*(Intentionally left blank)*

41. I further request that the Court authorize execution of the warrant at any time of day or night, owing to the potential need to locate the Target Cell Phone outside of daytime hours.

Respectfully submitted,

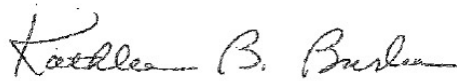


---

Andrew J. Eilerman/FBI Special Agent

8th

Sworn to via telephone on this \_\_\_\_\_ day of February, 2021  
after submission by reliable electronic means.  
Fed.R.Crim.P. 4.1 and 41(d)(3).



Kathleen B. Burke, U.S. Magistrate Judge